



Cryptshare for Outlook User Guide

V1.6.2

Befine Solutions AG
Werthmannstr. 15
79098 Freiburg i. Br.
Germany

Web: <https://www.cryptshare.com>
E-Mail: info@cryptshare.com
Tel.: +49 761 389 13 0
Fax: +49 761 389 13 115

1. Table of Contents

1.	Table of Contents	2
2.	First-time use	3
2.1.	Cryptshare Settings.....	3
2.1.1.	Your Name.....	3
2.1.2.	Phone no.....	3
2.1.3.	URL.....	3
2.1.4.	Proxy Settings.....	4
2.1.5.	Show filenames in notifications	4
2.1.6.	I want to be informed about downloads	4
2.1.7.	in this language	4
2.1.8.	Keep a copy of transferred files in the “sent items” folder	4
2.2.	Verification	5
2.2.1.	Automatic verification	5
2.2.2.	Manual Verification using the sidebar	7
2.2.3.	Manual Verification using the Cryptshare settings	8
3.	Sending files or messages encrypted via Cryptshare	11
3.1.	Creating a message	11
3.2.	Sending a message.....	11
3.3.	Defining transfer options	12
3.3.1.	Contents to be transferred encrypted	12
3.3.2.	Expiration date	13
3.3.3.	Set password options	14
3.3.4.	Notification options.....	16
3.4.	Monitor transfers	16
4.	Retrieve files	18

2. First-time use

After the plug-in is installed on your workstation, a few settings have to be made before you can start using the tool.

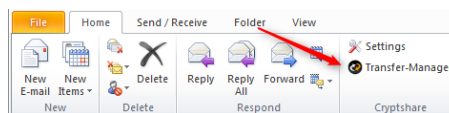
Your administrator has possibly made the majority of the settings already. However, you should check your name and phone number in the Cryptshare Settings in every case, as this information is passed on to the recipient of your transfers.

Further, it is necessary to perform a verification of your e-mail address which typically takes place automatically.

Both processes are described in the following chapters.

2.1. Cryptshare Settings

In the Outlook base screen there is a button with which you can change the settings of Cryptshare for Outlook.



Using this settings dialog, you can enter your name and telephone number for the notification of the recipient, define the settings for the connection to your Cryptshare server and the default behavior of the Cryptshare for Outlook plug-in. Please note that depending on administrative settings some of the options shown here may already be filled in, hidden or inactive.

Please check all the settings before using the plug-in. Eventually the Cryptshare “Settings” button is not visible to you at all. In this case, all settings are pre-defined by the administrator and there is no way to change them in the user interface.

2.1.1. Your Name

Please put your name in here. Your name will be shown to the recipient of the transfer.

2.1.2. Phone no

Please put your phone number in here. Your phone number will be displayed to the recipient of the transfer to enable him to get in touch with you.

2.1.3. URL

Please enter the URL of your Cryptshare server. After entering the URL, a connection test is performed automatically and you can see if the Cryptshare Server could be reached. Should this connection test fail, please check the URL and your Proxy Settings.

2.1.4. Proxy Settings

If you have to go through a proxy server to establish connection to the Cryptshare server, you can define the connection details and credentials for the proxy server here. Click the button "Proxy Settings"

2.1.4.1. [Use proxy settings](#)

If you need to login to your proxy server explicitly, please check this option.

2.1.4.2. [HTTP](#)

Please enter the proxy server URL here.

2.1.4.3. [Port](#)

Please enter the correct port number for the connection to the proxy server.

2.1.4.4. [Username](#)

Please enter the username for your proxy login.

2.1.4.5. [Password](#)

Please enter the password for your proxy login.

2.1.5. Show filenames in notifications

When you create a message and decide to only send the attachments via Cryptshare you can chose whether or not you would like to display the names of the sent files in your e-mail message. It might make sense to hide these as your message text is sent as unencrypted e-mail in this case and the filenames might already contain confidential information.

This setting allows you to specify a standard behaviour. You can still change this parameter for each transfer individually in the transfer options dialogue that comes up when you send your message.

2.1.6. I want to be informed about downloads

Here you can choose if you want to be notified by e-mail when a recipient of your message downloads the information provided for him.

2.1.7. in this language

This option allows you to set the language in which you would like to receive the download confirmation.

2.1.8. Keep a copy of transferred files in the "sent items" folder

This option allows you to specify whether you want to put the emails in the "Sent Items" folder along with the attachments, or whether you want the files removed and replaced by the file names before filing the email.

Retaining copies of the sent files in the "Sent Items" folder may slow down or even overload the e-mail system over time. Since very large amounts of data can be sent using Cryptshare for Outlook, there are certain limits for the storage of attachments.

There is a warning threshold and an absolute upper limit for attachments to be stored that apply even when you decide to save the e-mails along with the attachments.

If the total size of your message is above the threshold, but still below the limit, you will be notified and can decide whether or not you would like to keep the attachments in your message in "sent items". The name of the removed file attachments are shown in the message in order to ensure traceability.

If the total size of your message exceeds the limit, the message will be filed in "sent items" without the attachments. The names of the removed attachments will be shown in the message to keep a record.

2.2. Verification

Before using Cryptshare for Outlook the first time a verification of your e-mail address needs to be performed. This is necessary both for Exchange as well as POP3 and IMAP accounts.

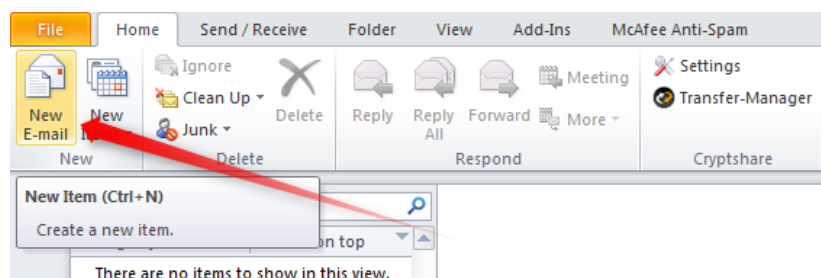
There is an automatic and a manual verification process. The way how the verification takes place is depending on the settings your administrator has made in this regard. Please note that IMAP email accounts cannot be verified automatically due to the implementation of IMAP in MS Outlook.

2.2.1. Automatic verification

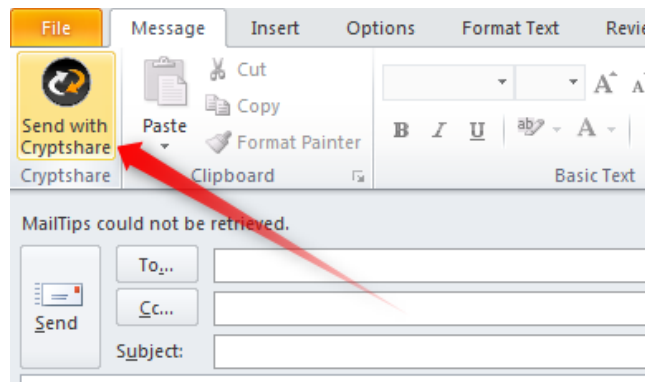
Automatic verification does not require any user interaction. Please be aware though that automatic verification can only be performed with MS Exchange and POP3 E-Mail accounts.

Please perform the following steps:

1. Create a new E-Mail



2. Click on "Send with Cryptshare"

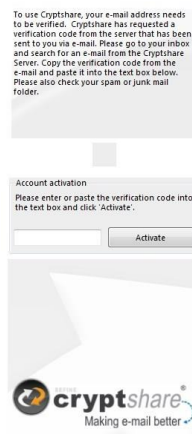


3. Cryptshare for Outlook requests a verification code via e-mail to your e-mail address. The plug-in monitors your inbox and junk folder for a pre-defined time and automatically processes the incoming code. In the meantime you will see an informational message in the sidebar.



If the automatic verification is successful, the sidebar will change and show the Cryptshare controls. Cryptshare is now ready for use.

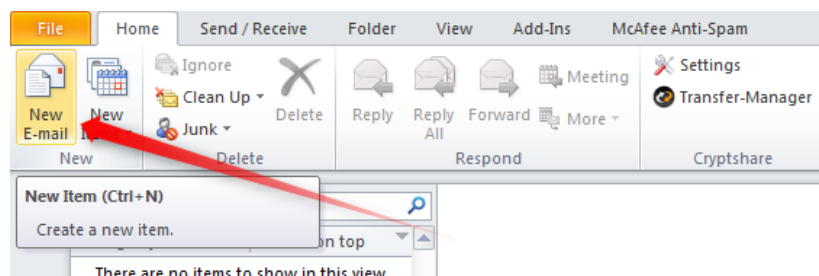
If automatic verification fails, you will be informed accordingly. Depending on the administrative settings, you will either be asked to get in touch with your administrator or you will have the possibility to enter a verification code manually. In this case, please check your inbox and junk mail folder manually for an e-mail coming from your Cryptshare server. Copy the verification code that you find in this e-mail into the clipboard and paste it into the field provided in the Cryptshare for Outlook sidebar.



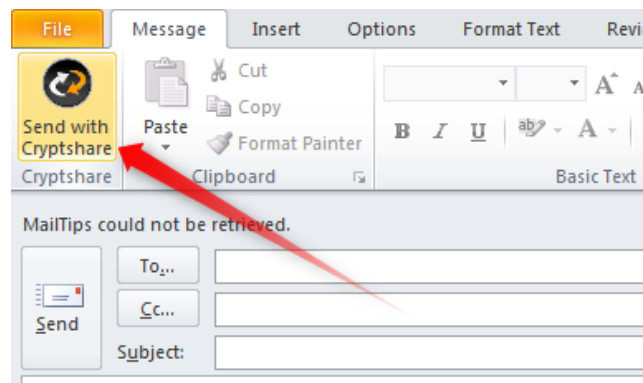
2.2.2. Manual Verification using the sidebar

Please perform the following steps:

1. Create a new E-Mail



2. Click on "Send with Cryptshare"

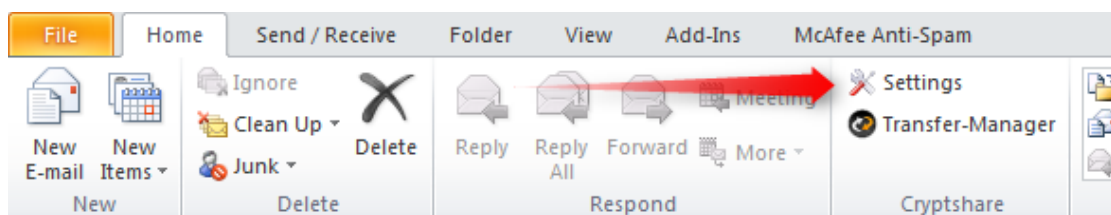


Cryptshare for Outlook requests a verification code via e-mail to your e-mail address. Please check your inbox and junk mail folder manually for an e-mail coming from your Cryptshare server. Copy the verification code that you find in this e-mail into the clipboard and paste it into the field provided in the Cryptshare for Outlook sidebar. The sidebar will change and show the Cryptshare controls. Cryptshare for Outlook is now ready for use.

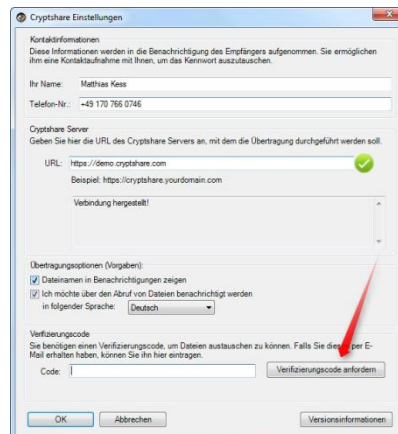
2.2.3. Manual Verification using the Cryptshare settings

If your administrator has set the manual verification mode, you can perform a verification at any time from the Cryptshare settings dialogue.

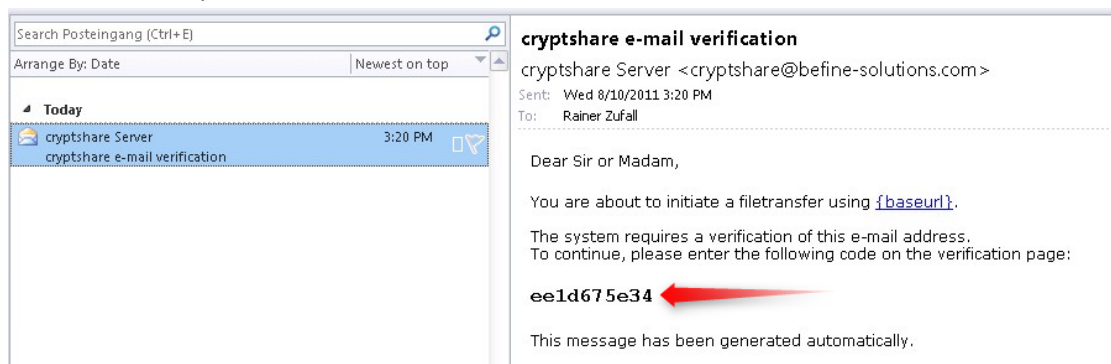
1. Open "Settings" from the Cryptshare Ribbon Tab on the MS Outlook main screen.



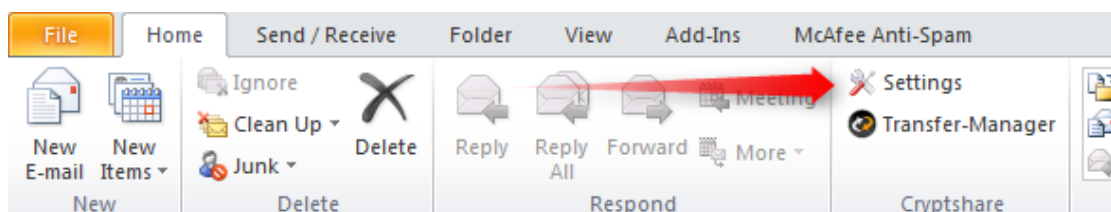
2. Click on "Request verification code". An e-mail containing a verification code will now be sent to your e-mail address. The following window informs about this process. Click on "Close / Go to Inbox"



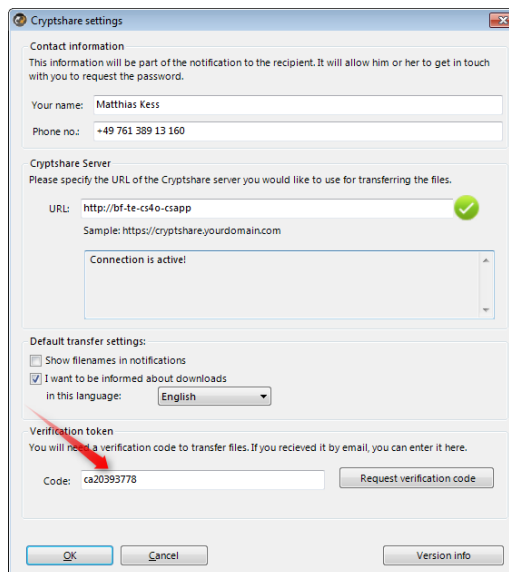
3. You will now find an e-mail containing a verification code in your inbox. Copy the verification code into the clipboard...



4. ...open Cryptshare Settings...



5. ...and paste the verification code into the field "Code" using the Ctrl+V keys.



The image shows the 'Cryptshare settings' dialog box. It has a title bar with a close button. The dialog is divided into several sections: 'Contact information' with fields for 'Your name' (Matthias Kess) and 'Phone no.' (+49 761 389 13 160); 'Cryptshare Server' with a 'URL' field (http://bf-te-cs4-o-csapp) and a 'Sample' field (https://cryptshare.yourdomain.com), followed by a 'Connection is active!' status box with a green checkmark; 'Default transfer settings' with checkboxes for 'Show filenames in notifications' (unchecked) and 'I want to be informed about downloads' (checked), and a language dropdown set to 'English'; and 'Verification token' with a 'Code' field (ca20393778) and a 'Request verification code' button. At the bottom are 'OK', 'Cancel', and 'Version info' buttons. A red arrow points to the 'Code' field.

Cryptshare settings

Contact information
This information will be part of the notification to the recipient. It will allow him or her to get in touch with you to request the password.

Your name: Matthias Kess
Phone no.: +49 761 389 13 160

Cryptshare Server
Please specify the URL of the Cryptshare server you would like to use for transferring the files.

URL: http://bf-te-cs4-o-csapp ✓
Sample: https://cryptshare.yourdomain.com

Connection is active!

Default transfer settings:

☐ Show filenames in notifications
☒ I want to be informed about downloads
in this language: English

Verification token
You will need a verification code to transfer files. If you received it by email, you can enter it here.

Code: ca20393778 Request verification code

OK Cancel Version info

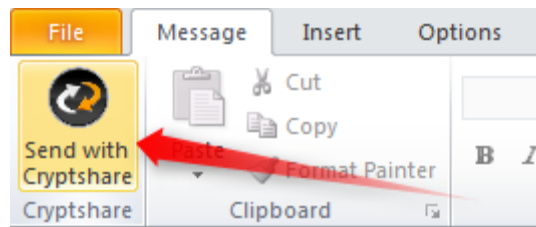
Cryptshare for Outlook is now ready for use.

3. Sending files or messages encrypted via Cryptshare

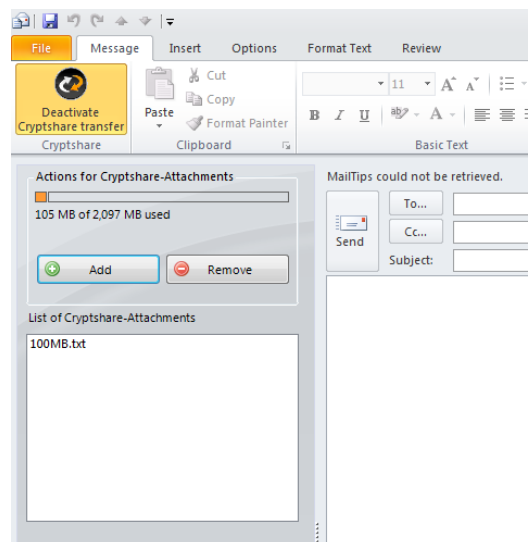
3.1. Creating a message

If you want to send files or a full message via Cryptshare, first create a new e-mail.

Within the e-mail screen, you can activate the mode "Send with Cryptshare" at any time.



The Cryptshare sidebar will now open. Using the "Add" button in the sidebar, you can attach files that exceed the size limit that is set in MS Outlook / MS Exchange.

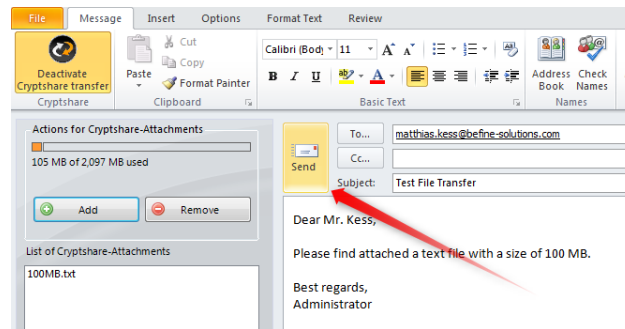


The Outlook button "Attach file" (paperclip symbol) is still active; however you can only add files that do not exceed the size limit configured in MS Outlook / MS Exchange using this button.

If you have already added files to your e-mail or if you add more files using the Outlook standard methods (button "Attach file" or drag & drop), these files will be moved over to the Cryptshare sidebar immediately.

3.2. Sending a message

When your message is ready to be sent, just click on the "Send" button of your Outlook Client as usual.



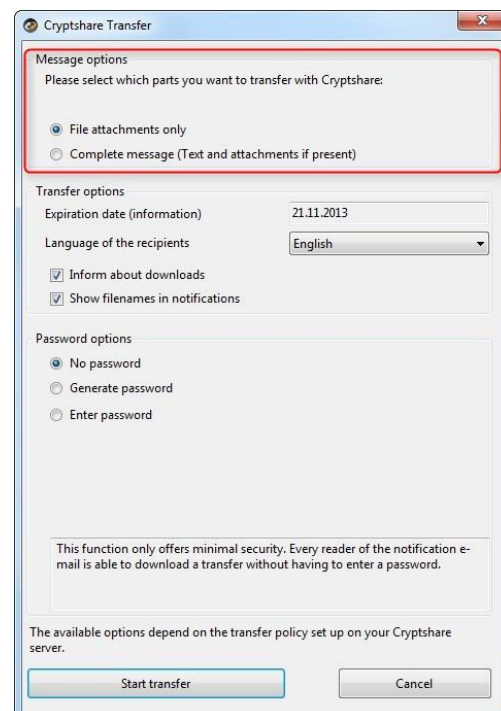
A window will pop up and you can now define transfer options.

3.3. Defining transfer options

Please note that depending on the administrative settings, some of the items described here may be pre-set, disabled or hidden on your workplace. Also the layout of the transfer options screen is depending on the version of the Cryptshare Server you communicate with (prior to V3.4.2.0 or V3.4.2.0 and higher). Below, both variants are described.

3.3.1. Contents to be transferred encrypted

You can select whether you want to transfer the complete message via Cryptshare or the file attachments only



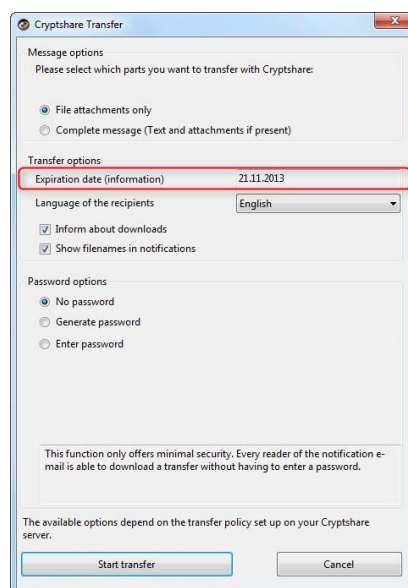
If you select "File attachments only", the attachments will be detached from your message and handed over to the Cryptshare server. Download information will be added to your message that can be used by the recipient to download the file(s).

If you want to send the complete message encrypted, a .eml file will be created out of your message and will be sent together with the file attachments via Cryptshare. In this case, the recipient will only receive a standard notification that contains all information required to download the files and the message available for him.

3.3.2. Expiration date

If you are connected to a Cryptshare Server V3.4.2.0 or higher, the expiration date of your transfer will be shown in the transfer settings dialogue. The date is shown for information only and cannot be changed.

If you are connected to a Cryptshare Server prior to V3.4.2.0, no information of the expiration date is shown.



Transfer expiration date

3.3.3. Set password options

3.3.3.1. When using a Cryptshare Server prior to V3.4.2.0



Password options using a Cryptshare Server prior to V3.4.2.0

If you decide to "use a password", you can define a password which will protect the transfer by means of encryption. In this case, you need to tell the recipient which password you have used. Cryptshare will send your contact details as defined in the Cryptshare settings to the recipient, so he or she can get in touch with you to ask for the password.

If you do not activate password protection, the file will still be sent encrypted. However the password will be generated automatically and will be sent unencrypted to the recipient as part of the download link. This option is significantly less secure as an unauthorized recipient of the e-mail message will be capable of getting access to files because it contains the link and the password. However the handling is much easier as sender and recipient do not need to exchange the password. This option is only recommended for transferring files which are too large for e-mail, but not confidential.

3.3.3.2. When using a Cryptshare Server V3.4.2.0 or higher

The image shows a 'Cryptshare Transfer' dialog box. It has three main sections: 'Message options' with radio buttons for 'File attachments only' (selected) and 'Complete message (Text and attachments if present)'; 'Transfer options' with a date field set to '21.11.2013', a language dropdown set to 'English', and two checked checkboxes: 'Inform about downloads' and 'Show filenames in notifications'; and 'Password options' with radio buttons for 'No password' (selected), 'Generate password', and 'Enter password'. A red rectangle highlights the 'Password options' section. Below this section is a warning text: 'This function only offers minimal security. Every reader of the notification e-mail is able to download a transfer without having to enter a password.' At the bottom, there are 'Start transfer' and 'Cancel' buttons, and a note: 'The available options depend on the transfer policy set up on your Cryptshare server.'

Password options when using a Cryptshare Server V3.4.2.0 or higher

The options that are available for setting a password are depending on the policies that the administrator has set up on server side and may vary from recipient to recipient.

No password

If you decide to use “No password”, the file will still be sent encrypted. However the password will be generated automatically and will be sent unencrypted to the recipient as part of the download link. This option is significantly less secure as an unauthorized recipient of the e-mail message will be capable of getting access to files because the message contains the link and the password. However the handling is much easier as sender and recipient do not need to deal with passwords at all. This option is only recommended for transferring files which are too large for e-mail, but not confidential.

Generate password

The system automatically generates a password that meets the qualitative requirements that the administrator has set for this combination of sender and recipient. **Important!** Please note the password or copy the password into the clipboard using the button next to the password field before you start the transfer. If you do not remember the password for data you have provided, the data cannot be downloaded and the password cannot be changed. The data will be deleted from the system after the date of expiry.

Enter password

Enter a password of your choice. The password needs to fulfil the qualitative requirements that the administrator has set. Icons underneath the password entry field show you which requirements you still have to fulfil before the password is accepted. You can use the button next to the password entry field to copy the password into the clipboard.

3.3.4. Notification options

3.3.4.1. Language of the recipients

You can select a language for the notification text to the recipient. This should typically be the language that you write your e-mail message in, as a standard text in the selected language will be added to your message text to inform the recipient about how to retrieve the files.

3.3.4.2. Inform about downloads

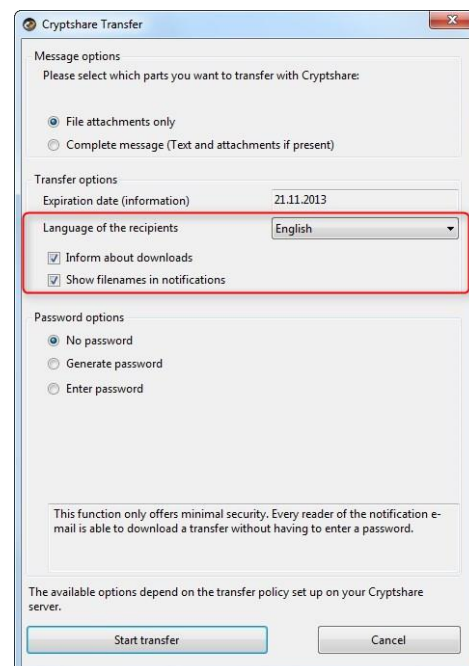
If you activate this option, you will be notified via e-mail if one of the recipients of your messages starts to download the files that you have provided.

3.3.4.3. Show filenames in notifications

If you activate this option, the file names will be listed in the notification to the recipient in plain text. You may want to deactivate this option if the file names contain a secret.



Notification options when using a Cryptshare Server prior to V3.4.2.0



Notifications options when using a Cryptshare Server V3.4.2.0 or higher

3.4. Monitor transfers

After clicking on "Start transfer", the Cryptshare Transfer Manager will open. Here you can monitor the progress of your Cryptshare transfers. Your message will remain in the "Drafts" folder while the files are being uploaded. Afterwards, the message will be put into the "Sent" folder.



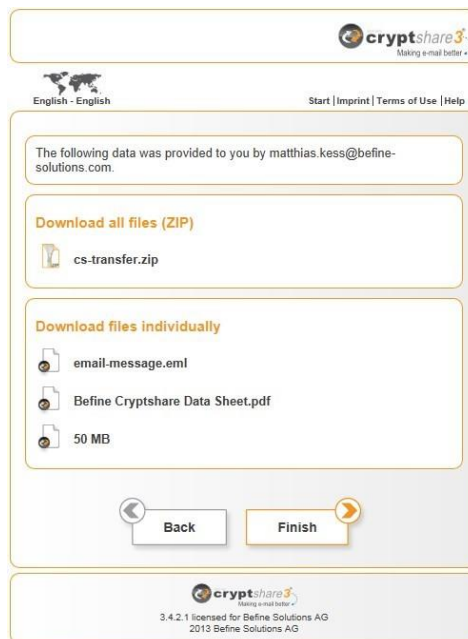
You can close the transfer manager at any time manually or you can activate the option "Close automatically if all transfers are completed". Also you can click on "Remove" to remove a single entry from the list. You can re-open the transfer manager at any time by clicking on "Transfer Manager" in the Cryptshare ribbon in the Outlook main screen.



4. Retrieve files

The recipients of your message either receive your original e-mail complemented by download information or a standardised notification message, depending on the options you have selected when sending. When they click the download link, the download area of the Cryptshare server will open in the browser so the recipient can retrieve the files.

If you have decided to send the complete message encrypted, you will find a file named "E-Mail message.eml" in the transfer package. This file contains the encrypted e-mail message that will open in the e-mail software for viewing.



This functionality is available for users of MS Outlook 2007, 2010, 2013, MS Outlook Express, MS Live Mail, IBM Lotus Notes Version 8 or higher, Mozilla Thunderbird. Other e-mail client software may not be able to open .eml files.

The files available can be downloaded individually or all together at once as zip archive, including the confidential message (Cryptshare 3 servers only).